

Hojas >	Ej.1	Ej.2	Ej.3	Ej.4	
	1	1	1	1	
Calif. >	B	B-	B-	R	<u>A</u>

Todas las respuestas se consideran válidas solo si están debidamente justificadas.

Ejercicio 1

Desde un host con dirección 192.168.100.55 se capturan los siguientes segmentos TCP:

No.	Source	Destination	Info
1	192.168.100.35	192.168.100.40	8443 > 33242 [ACK] Seq=50 Ack=110 Len=0
2	192.168.100.40	192.168.100.35	33242 > 8443 [ACK] Seq=110 Ack=50 Len=80
3	192.168.100.35	192.168.100.40	8443 > 33242 [ACK] Seq=50 Ack=190 Len=10
4	192.168.100.40	192.168.100.35	33242 > 8443 [FIN,ACK] Seq=190 Ack=50 Len=0
5	192.168.100.35	192.168.100.40	8443 > 33242 [FIN,ACK] Seq=60 Ack=190 Len=0
6	192.168.100.35	192.168.100.40	8443 > 33242 [ACK] Seq=61 Ack=191 Len=0
7	192.168.100.40	192.168.100.35	33242 > 8443 [ACK] Seq=191 Ack=61 Len=0

- Indicar una posible secuencia de estados TCP atravesados por cada socket que se pueda deducir a partir de la captura explicando los cambios de estados que produce cada paquete.
- Completar la captura con una posible secuencia de segmentos previos a los capturados desde que comienza el establecimiento de la conexión. Suponer que ambos extremos de la conexión no realizan más envíos de segmentos con datos que los que aparecen en la captura y que el host 192.168.100.35 comienza en el estado LISTEN.

Ejercicio 2

Por falta de datos, una conexión RTT=100ms, Ssthresh=24KB y CWND=64KB dejó de transmitir por 150ms. En ese instante, recibe de la capa superior 64KB nuevos para enviar y durante todo el envío el receptor anuncia una *Advertised Window* de 22KB.

- Muestre para cada RTT los valores de las variables más relevantes del control de congestión de TCP para la transmisión completa de los nuevos datos. Suponiendo que no se producen errores, ¿Cuánto tiempo tarda la conexión en enviar los datos?
- Ahora bien, suponga que el último ACK que envía el receptor en el inciso anterior, tenía prendido el flag de RESET, pero desde la capa de aplicación todavía se necesitan enviar 100KB adicionales. En este nuevo escenario, se sabe que el receptor siempre anuncia una *Advertised Window* de 22KB, hasta que recibe 32KB de datos y a partir de ese momento la *Advertised Window* que anuncia se duplica por cada RTT. Suponiendo que no se producen errores, ¿Cuánto tiempo demandará completar la transferencia? ¿Cuál es el valor de la variable CWND al recibir el último ACK?
- (Conceptual) ¿Cuál es la desventaja de usar Fast Retransmit/Fast Recovery en una conexión que pasa por una red que desordena muchos paquetes?

Ejercicio 3

Una compañía debe exponer un servicio Web a Internet separándolo de su red interna mediante un firewall *Stateful*. Este servicio se implementa usando un único servidor que responde peticiones HTTP y HTTPS, al que a su vez, se necesita acceder desde la red interna usando SSH. Además, para la red interna se permite acceder al servicio Web mencionado previamente, así como a otros sitios Web en Internet, usando HTTP y HTTPS. Todas las consultas DNS de la red interna deben hacerse a un servidor DNS en Internet con dirección IP 8.8.8.8.

- Diagrama un esquema de conectividad mostrando cómo organizar la red usando una zona demilitarizada (DMZ) y muestre las reglas del firewall.
- Los usuarios en la red interna quieren acceder al servidor por SSH pero sin tener que escribir su contraseña, muestre cómo deberían instalarse las claves para que el servicio SSH pueda garantizar la autenticidad de cada usuario.

Ejercicio 4

Dado el siguiente fragmento de la base de datos de un servidor DNS autoritativo para el dominio uba.ar y la siguiente secuencia de peticiones HTTP realizadas por un mismo navegador en una PC con nombre gorrión.uba.ar.:

Base de datos DNS

```
...
uba.ar.      IN  NS      ns1.uba.ar
uba.ar.      IN  NS      ns2.uba.ar
uba.ar.      IN  MX      5 smtp1.uba.ar
uba.ar.      IN  MX      15 celeste.dc.uba.ar
rectorado    IN  CNAME   secretaria.uba.ar
alumnos      IN  CNAME   secretaria.uba.ar
ns1           IN  A        208.25.19.1
ns2.uba.ar.  IN  A        208.25.19.3
secretaria   IN  A        208.25.19.87
gorrión      IN  A        208.25.19.2
smtp1.uba.ar IN  A        208.25.19.99
smtp2        IN  A        208.25.19.55
...
```

Peticiones HTTP

```
GET /logo.jpg HTTP/1.1
Host: secretaria.uba.ar
User-agent: Mozilla/4.0
Accept-Language: es
...

GET /logo.jpg HTTP/1.1
Host: rectorado.uba.ar
User-agent: Mozilla/4.0
Accept-Language: es
...
```

Se pide:

- ¿Los encabezados de las respuestas son necesariamente iguales? ¿Las imágenes son necesariamente iguales? Explicar.
- Muestre las conexiones TCP involucradas en las peticiones HTTP en el siguiente formato:
<ip origen, puerto origen, ip destino, puerto destino>
- En el instante t_0 un usuario desde su PC en algún lugar de Internet envía un correo electrónico a la dirección `rector@uba.ar`. En ese mismo instante todos los servidores SMTP receptores del dominio se encuentran apagados por mantenimiento. Indique cuáles son esos servidores y sus direcciones IP si las conoce. ¿Qué ocurre con el mensaje de correo enviado?

1. Al no haber capturado ningún paquete con flag S encendido se puede asumir que ambos sockets están en estado ESTABLISHED. Por lo tanto los primeros 3 paquetes son el envío de datos entre ambos.

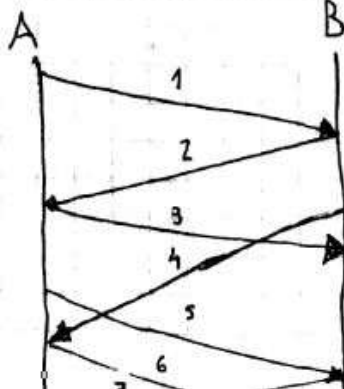
Ahora bien, el paquete 4 contiene el flag F encendido, pero no reconoce el paquete de datos enviado por A (192.168.100.35) por lo tanto B (192.168.100.40) debe haber recibido un señal de cierre interno, por lo que pasa a FIN-WAIT-1.

Luego, el paquete número 6, de A a B, también tiene encendido el flag F, lo cual ~~debe~~ no debe haber recibido el paquete 4, sino que ante recibir un señal Close, por lo tanto A pasa a FIN-WAIT-1.

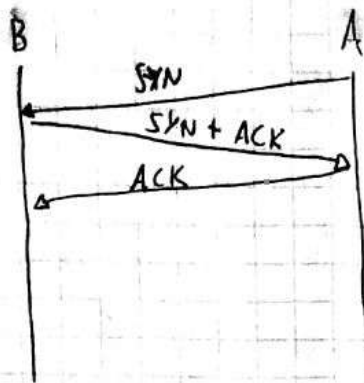
En el sexto paquete A envía A encendido, lo cual surge al recibir el FIN de B, ya que se ve en la modificación del campo seq y ack, entonces A pasa a CLOSING.

Finalmente B responde con A al FIN enviado por A y también pasa a CLOSING. Como ambos envían las respectivas ACK, si ~~se~~ se supusiera que no se pierden, al momento que los reciben pasaran a TIME-WAIT y luego a CLOSED.

DIAGRAMA:



b) DIAGRAMA:



Como el primer mensaje visto en la captura es de A a B enviándole un ACK y se pide que A este en LISTEN y que no haya una de datos, entonces una posible secuencia es la mostrada en el diagrama. En donde ambos estaban en estado LISTEN. A genera un paquete SYN, pasa a SYN_SENT. B recibe el SYN para o SYN_RCVD y envía un SYN+ACK. Luego se ve el primer paquete capturado en donde A pasa a ESTABLISHED al recibir el ACK y B también llega a ESTABLISHED al recibir el ACK.

Luego los paquetes serán:

192.168.100.35 192.168.100.40

192.168.100.40 192.168.100.35

1° PAQUETE ENUNCIADO ...

[SYN] seq=49 len=0

[SYN+ACK] seq=109 ACK=50 len=0

2) $RTT = 100 \text{ ms}$ $SSTHRESH = 24 \text{ Kb}$ $CWND = 64 \text{ Kb}$

$RTO = 2 \cdot RTT = 200 \text{ ms}$

$RWND = 22 \text{ Kb}$

Caso el envío del nuevo paquete de 64 Kb llega a los 150 ms, entonces no se llega a completar un RTO ^{Luego} los valores anteriores se mantienen.
Luego:

SIN TRANSMITIR

RTT	CWND	RWND	SSTHRESH	FLIGHT SIZE	LS
1	64 Kb	22 Kb	24 Kb	22 Kb	22 Kb
2	66 Kb	22 Kb	24 Kb	22 Kb	44 Kb
3	68 Kb	22 Kb	24 Kb	20 Kb	64 Kb
4					

La conexión tardará 400 ms en enviar los datos.

b) Como el último ACK enviado por el receptor contiene el flag Reset encendido, debemos comenzar con los valores predeterminados los 100 Kb restantes.

Estos son $CWND = 4 \text{ Kb}$ $SSTHRESH = 64 \text{ Kb}$



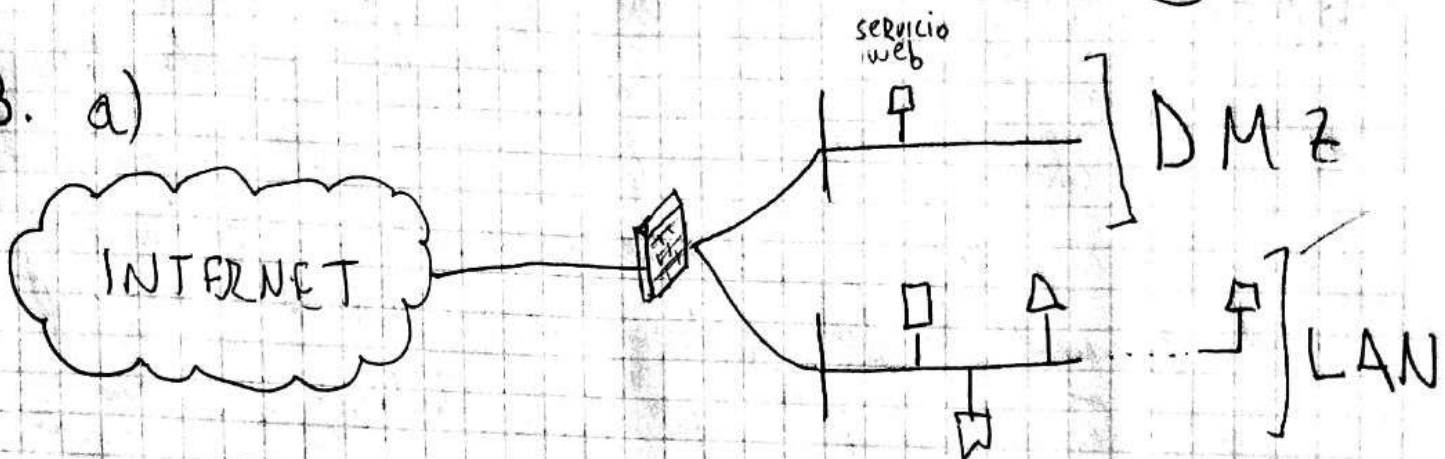
RTT	CWND	RWND	SSTHRESH	FLIGHTSIZE	LBS
1	4 Kb	22 Kb	64 Kb	4 Kb	4 Kb
2	8 Kb	22 Kb	64 Kb	8 Kb	12 Kb
3	16 Kb	22 Kb	64 Kb	16 Kb	28 Kb
4	32 Kb	22 Kb	64 Kb	22 Kb	50 Kb
5	76 Kb ^{66 Kb}	44 Kb ^{44 Kb}	64 Kb	44 Kb	94 Kb
6	79 Kb ^{76 Kb}	88 Kb	64 Kb	6 Kb	100 Kb
7	80 Kb	176 Kb	64 Kb	—	100 Kb

- SACKS (Slow Start) + (SACK CA)
- El RWND comienza a duplicarse en el RTT 5 ya que cuando recibe los datos de la cuarta ventana llega a 32 Kb y supera. Luego comienza duplicándose.
 - En el 6 el CWND aumenta por CA $\Rightarrow CWND = CWND_{[i-1]} + \frac{SSTHRESH}{CWND_{[i-1]}} * Ack$
 $\Rightarrow CWND = 76 Kb + \frac{4 Kb}{76 Kb} * 44 \approx 76 Kb + 2.3 Kb \approx 79 Kb$
 - Luego en 7 $CWND \approx 79 Kb + 0.3 Kb \approx 80 Kb$

Por lo tanto la transmisión de los 100 Kb tarda 100 ms y el CWND finaliza con 80 Kb.

c) El problema de usar FR/FR en una conexión que pare por una red que desordena muchos paquetes, es que se recibirán muchos ACKS duplicados por el problema, y esto causará un incremento mayor de la ventana del emisor, lo que seguirá congestionando la red innecesariamente.

3. a)



HASTA DESDE	LAN	DMZ	INTERNET
LAN	 	HTTP/HTTPS SSH	HTTP/HTTPS DNS
DMZ	DROP	 	DROP
INTERNET	DROP	HTTP/HTTPS	

Luego las reglas del FIREWALL son: (Suponiendo mismas puertos)
HTTP/HTTPS

< LAN, *, DMZ, Puerto HTTP/s, TCP > ✓ OK, REPO SERV

< LAN, *, INTERNET, Puerto HTTP/s, TCP > IDEM

< LAN, *, INTERNET, Puerto DNS, UDP > ✓
8.8.8.8

< INTERNET, *, DMZ, Puerto HTTP/s, TCP > ✓

ALTA SSH

b) Para que las urnas no deban ser escritas en contra de
por conectar al servidor, el servidor debe tener presente instalada
todas las claves públicas de los usuarios, de este modo las
urnas se conectarán con SSH encriptando con su respectiva clave
privada en ~~una~~ identidad y luego el servidor debe descifrar
con la respectiva clave pública para poder autenticar la conexión.

4) a) Las cabeceras de las requestas no son iguales,
ya que la primera sera de 2XX SUCCES ya que ^{puede} no llegar
directamente desde la base DNS.

Mientras que la segunda comprende o una redirección
ya que la entrada de redirección en los registros DNS se redirecciona a
secretaria.UBA.AR.

Entonces, por esto ultimo la imagen siempre sera la misma ya que
se tardará del mismo lugar. Son servidores virtuales $\neq 5$

b. 1. $\langle 208.25.19.2, 80, 208.25.19.87, 80 \rangle$
2. $\langle 208.25.19.2, 80, 208.25.19.87, 80 \rangle$

71024
*

1 solo CX
x 6/HTTP/1.1

(C.)



c) Al momento que el usuario envía el correo a rector@uba.ar. primero se lo envió a su servidor SMTP, el cual debe tener su dirección, sin cancelarlo.

Luego el servidor SMTP de este usuario ~~hace~~ hace un pedido DNS de Tipo MX ~~para~~ uba.ar. por lo que llega a la tabla DNS del enunciado, y esto tabla se responde con las líneas con MX.

Uno vez obtenido intento de obtener la IP ~~del~~ que tiene la menor prioridad, esto es SMTP1.UBA.AR.

~~Vuélve~~ Envío un request SMTP1.UBA.AR. A con donde vuelve a llegar a la tabla DNS y se responde 208.25.19.99.

Intento de enviar el mail pero al estar caído el servidor no obtiene respuesta, por lo tanto intento con la segunda dirección.

Vuelve a enviar a la base de datos DNS un request con CELESTE.DC.UBA.AR. A ~~aguarda respuesta~~ al no tener la respuesta se responde que busquen en NS1.UBA.AR o en NS2.UBA.AR, luego no se sabe que obtendrá

"	"
208.25.19.1	208.25.19.3

pero se puede saber que no podrá ser enviado el correo

se envía
al servidor